EXHIBIT A

Randomness

From Wikipedia, the free encyclopedia
(Redirected from Random)

Randomness is a concept of non-order or non-coherence in a sequence of symbols or steps, such that there is no intelligible pattern or combination. Randomness has somewhat disparate meanings as used in several different fields. It also has common meanings which may have loose connections with some of those more definite meanings. The Oxford English Dictionary defines "random" thus:

> Having no definite aim or purpose; not sent or guided in a particular direction; made, done, occurring, etc., without method or conscious choice; haphazard.

Also, in statistics, as:

> Governed by or involving equal chances for each of the actual or hypothetical members of a population; (also) produced or obtained by such a process, and therefore unpredictable in detail.

Closely connected, therefore, with the concepts of chance, probability, and information entropy, randomness implies a lack of predictability. More formally, in statistics, a random process is a repeating process whose outcomes follow no describable deterministic pattern, but follow a probability distribution, such that the relative probability of the occurrence of each outcome can be approximated or calculated. For example, the rolling of a fair six-sided die in neutral conditions may be said to produce random results, because one cannot compute, before a roll, what number will show up. However, the probability of rolling any one of the six rollable numbers can be calculated, assuming that each is equally likely.

The term is often used in statistics to signify well-defined statistical properties, such as a lack of bias or correlation. Monte Carlo Methods, which rely on random input, are important techniques in science, as, for instance, in computational science.[1] Random selection is an official method to resolve tied elections in some jurisdictions[2] and is even an ancient method of divination, as in tarot, the I Ching, and bibliomancy. Its use in politics is very old, as office holders in Ancient Athens were chosen by lot, there being no voting.

Contents

History

Main article: History of randomness

In ancient history, the concepts of chance and randomness were intertwined with that of fate. Many ancient peoples threw dice to determine fate, and this later evolved into games of chance. Most ancient cultures used various methods of divination to attempt to circumvent randomness and fate.[3][4]

The Chinese were perhaps the earliest people to formalize odds and chance 3,000 years ago. The Greek philosophers discussed randomness at length, but only in non-quantitative forms. It was only in the sixteenth century that Italian mathematicians began to formalize the odds associated with various games of chance.

Ancient fresco of dice players in Pompei.

The invention of the calculus had a positive impact on the formal study of randomness. In the 1888 edition of his book *The Logic of Chance* John Venn wrote a chapter on "The conception of randomness" which included his view of the randomness of the digits of the number Pi by using them to construct a random walk in two dimensions.[5]

The early part of the twentieth century saw a rapid growth in the formal analysis of randomness, as various approaches for a mathematical foundations of probability were introduced. In the mid to late twentieth century ideas of algorithmic information theory introduced new dimensions to the field via the concept of algorithmic randomness.

Although randomness had often been viewed as an obstacle and a nuisance for many centuries, in the twentieth century computer scientists began to realize that the *deliberate* introduction of randomness into computations can be an effective tool for designing better algorithms. In some cases such randomized algorithms outperform the best deterministic methods.

Randomness in science

Many scientific fields are concerned with randomness:

- Algorithmic probability
- Chaos theory

- Cryptography
- Game theory
- Information theory
- Pattern recognition
- Probability theory
- Quantum mechanics
- Statistics
- Statistical mechanics

In the physical sciences

In the 19th century, scientists used the idea of random motions of molecules in the development of statistical mechanics in order to explain phenomena in thermodynamics and the properties of gases.

According to several standard interpretations of quantum mechanics, microscopic phenomena are objectively random[*citation needed*]. That is, in an experiment where all causally relevant parameters are controlled, there will still be some aspects of the outcome which vary randomly. An example of such an experiment is placing a single unstable atom in a controlled environment; it cannot be predicted how long it will take for the atom to decay; only the probability of decay within a given time can be calculated.[6] Thus, quantum mechanics does not specify the outcome of individual experiments but only the probabilities. Hidden variable theories are inconsistent with the view that nature contains irreducible randomness: such theories posit that in the processes that appear random, properties with a certain statistical distribution are somehow at work "behind the scenes" determining the outcome in each case.

In biology

The modern evolutionary synthesis ascribes the observed diversity of life to natural selection, in which some random genetic mutations are retained in the gene pool due to the *non-random* improved chance for survival and reproduction that those mutated genes confer on individuals who possess them.

The characteristics of an organism arise to some extent deterministically (e.g., under the influence of genes and the environment) and to some extent randomly. For example, the *density* of freckles that appear on a person's skin is controlled by genes and exposure to light; whereas the exact location of *individual* freckles seems to be random.[7]

Randomness is important if an animal is to behave in a way that is unpredictable to others. For instance, insects in flight tend to move about with random changes in direction, making it difficult for pursuing predators to predict their trajectories.

In mathematics

The mathematical theory of probability arose from attempts to formulate mathematical descriptions of chance events, originally in the context of gambling, but later in connection with physics. Statistics is used to infer the underlying probability distribution of a collection of empirical observations. For the purposes of simulation, it is necessary to have a large supply of random numbers or means to generate them on demand.

Algorithmic information theory studies, among other topics, what constitutes a random sequence. The central idea is that a string of bits is random if and only if it is shorter than any computer program that

can produce that string (Kolmogorov randomness)—this means that random strings are those that cannot be compressed. Pioneers of this field include Andrey Kolmogorov and his student Per Martin-Löf, Ray Solomonoff, and Gregory Chaitin.

In mathematics, there must be an infinite expansion of information for randomness to exist. This can best be seen with an example. Given a random sequence of three-bit numbers, each number can have only eight possible values:

000, 001, 010, 011, 100, 101, 110, 111

Therefore, as the random sequence progresses, it must recycle through the values it previously used. In order to increase the information space, another bit may be added to each possible number, giving 16 possible values from which to pick a random number. It could be said that the random four-bit number sequence is more random than the three-bit one. This suggests that in order to have true randomness, there must be an infinite expansion of the information space.

Randomness is said to occur in numbers such as log (2) and Pi. The decimal digits of Pi constitute an infinite sequence and "never repeat in a cyclical fashion". Numbers like pi are also thought to be normal, which means that their digits are random in a certain statistical sense.

> Pi certainly seems to behave this way. In the first six billion decimal places of pi, each of the digits from 0 through 9 shows up about six hundred million times. Yet such results, conceivably accidental, do not prove normality even in base 10, much less normality in other number bases.[8]

In information science

In information science, irrelevant or meaningless data is considered to be noise. Noise consists of a large number of transient disturbances with a statistically randomized time distribution.

In communication theory, randomness in a signal is called "noise" and is opposed to that component of its variation that is causally attributable to the source, the signal.

In finance

The random walk hypothesis considers that asset prices in an organized market evolve at random.

Other so-called random factors intervene in trends and patterns to do with supply-and-demand distributions. As well as this, the random factor of the environment itself results in fluctuations in stock and broker markets.

Randomness versus unpredictability

Randomness, as opposed to unpredictability, is held to be an objective property - determinists believe it is an *objective* fact that randomness does not in fact exist. Also, what *appears* random to one observer may not appear random to another. Consider two observers of a sequence of bits, when only one of whom has the cryptographic key needed to turn the sequence of bits into a readable message. For that observer the message is not random, but it is unpredictable for the other.

One of the intriguing aspects of random processes is that it is hard to know whether a process is truly random. An observer may suspect that there is some "key" that unlocks the message. This is one of the

foundations of superstition, and is also a motivation for discovery in science and mathematics.

Under the cosmological hypothesis of determinism, there is no randomness in the universe, only unpredictability, since there is only one possible outcome to all events in the universe. A follower of the narrow frequency interpretation of probability could assert that no event can be said to have probability, since there is only one universal outcome. On the other hand, under the rival Bayesian interpretation of probability there is no objection to the use of probabilities in order to represent a lack of complete knowledge of the outcomes.

Some mathematically defined sequences, such as the decimals of pi mentioned above, exhibit some of the same characteristics as random sequences, but because they are generated by a describable mechanism, they are called *pseudorandom*. To an observer who does not know the mechanism, a pseudorandom sequence is unpredictable.

Chaotic systems are unpredictable in practice due to their extreme sensitivity to initial conditions. Whether or not they are unpredictable in terms of computability theory is a subject of current research. At least in some disciplines of computability theory, the notion of randomness is identified with computational unpredictability.

Individual events that are random may still be precisely described *en masse*, usually in terms of probability or expected value. For instance, quantum mechanics allows a very precise calculation of the half-lives of atoms even though the process of atomic decay is random. More simply, although a single toss of a fair coin cannot be predicted, its general behavior can be described by saying that if a large number of tosses are made, roughly half of them will show up heads. Ohm's law and the kinetic theory of gases are non-random macroscopic phenomena that are assumed to be random at the microscopic level.

Randomness and religion

Some theologians have attempted to resolve the apparent contradiction between an omniscient deity, or a first cause, and free will using randomness. Discordians have a strong belief in randomness and unpredictability. Buddhist philosophy states that any event is the result of previous events (karma), and as such, there is no such thing as a random event or a first event.

Martin Luther, the forefather of Protestantism, believed that there was nothing random based on his understanding of the Bible. As an outcome of his understanding of randomness, he strongly felt that free will was limited to low-level decision making by humans. Therefore, when someone sins against another, decision making is only limited to how one responds, preferably through forgiveness and loving actions. He believed, based on Biblical scripture, that humans cannot will themselves faith, salvation, sanctification, or other gifts from God. Additionally, the best people could do, according to his understanding, was not sin, but they fall short, and free will cannot achieve this objective. Thus, in his view, absolute free will and unbounded randomness are severely limited to the point that behaviors may even be patterned or ordered and not random. This is a point emphasized by the field of behavioral psychology.

These notions and more in Christianity often lend to a highly deterministic worldview and that the concept of random events is not possible. Especially, if purpose is part of this universe, then randomness, by definition, is not possible. This is also one of the rationales for religious opposition to evolution, where, according to theory, (non-random) selection is applied to the results of random genetic variation.

Donald Knuth, a Stanford computer scientist and Christian commentator, remarks that he finds pseudorandom numbers useful and applies them with purpose. He then extends this thought to God who may use randomness with purpose to allow free will to certain degrees. Knuth believes that God is interested in people's decisions and limited free will allows a certain degree of decision making. Knuth, based on his understanding of quantum computing and entanglement, comments that God exerts dynamic control over the world without violating any laws of physics, suggesting that what appears to be random to humans may not, in fact, be so random.[9]

C. S. Lewis, a 20th-century Christian philosopher, discussed free will at length. On the matter of human will, Lewis wrote: "God willed the free will of men and angels in spite of His knowledge that it could lead in some cases to sin and thence to suffering: i.e., He thought freedom worth creating even at that price." In his radio broadcast, Lewis indicated that God "gave [humans] free will. He gave them free will because a world of mere automata could never love..."

In some contexts, procedures that are commonly perceived as randomizers—drawing lots or the like — are used for divination, e.g., to reveal the will of the gods; see e.g. Cleromancy.

Applications and use of randomness

Main article: Applications of randomness

In most of its mathematical, political, social and religious use, randomness is used for its innate "fairness" and lack of bias.

Political: Greek Democracy was based on the concept of isonomia (equality of political rights) and used complex allotment machines to ensure that the positions on the ruling committees that ran Athens were fairly allocated. Allotment is now restricted to selecting jurors in Anglo-Saxon legal systems and in situations where "fairness" is approximated by randomization, such as selecting jurors and military draft lotteries.

Social: Random numbers were first investigated in the context of gambling, and many randomizing devices, such as dice, shuffling playing cards, and roulette wheels, were first developed for use in gambling. The ability to produce random numbers fairly is vital to electronic gambling, and, as such, the methods used to create them are usually regulated by government Gaming Control Boards. Random drawings are also used to determine lottery winners. Throughout history, randomness has been used for games of chance and to select out individuals for an unwanted task in a fair way (see drawing straws).

Sports: Some sports, including American Football, use coin tosses to randomly select starting conditions for games or seed tied teams for postseason play. The National Basketball Association uses a weighted lottery to order teams in its draft.

Mathematical: Random numbers are also used where their use is mathematically important, such as sampling for opinion polls and for statistical sampling in quality control systems. Computational solutions for some types of problems use random numbers extensively, such as in the Monte Carlo method and in genetic algorithms.

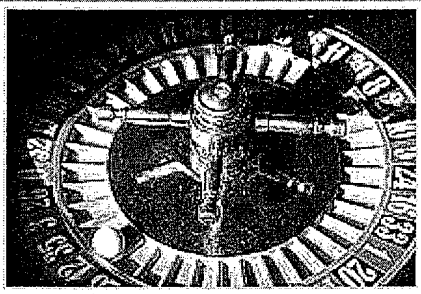
Medicine: Random allocation of a clinical intervention is used to reduce bias in controlled trials (e.g., randomized controlled trials).

Religious: Although not intended to be random, various forms of divination such as cleromancy see

what appears to be a random event as a means for a divine being to communicate their will. (See also Free will and Determinism).

Generating randomness

Main article: Random number generation



The ball in a roulette can be used as a source of apparent randomness, because its behavior is very sensitive to the initial conditions.

It is generally accepted that there exist three mechanisms responsible for (apparently) random behavior in systems:

1. *Randomness* coming from the environment (for example, Brownian motion, but also hardware random number generators)
2. *Randomness* coming from the initial conditions. This aspect is studied by chaos theory and is observed in systems whose behavior is very sensitive to small variations in initial conditions (such as pachinko machines, dice ...).
3. *Randomness* intrinsically generated by the system. This is also called pseudorandomness and is the kind used in pseudo-random number generators. There are many algorithms (based on arithmetics or cellular automaton) to generate pseudorandom numbers. The behavior of the system can be determined by knowing the seed state and the algorithm used. These methods are quicker than getting "true" randomness from the environment.

The many applications of randomness have led to many different methods for generating random data. These methods may vary as to how unpredictable or statistically random they are, and how quickly they can generate random numbers.

Before the advent of computational random number generators, generating large amounts of sufficiently random numbers (important in statistics) required a lot of work. Results would sometimes be collected and distributed as random number tables.

Randomness measures and tests

There are many practical measures of randomness for a binary sequence. These include measures based on frequency, discrete transforms, and complexity, or a mixture of these. These include tests by Kak, Phillips, Yuen, Hopkins, Beth and Dai, Mund, and Marsaglia and Zaman.[10]

Links related to generating randomness

- Hardware random number generator
- Entropy (computing)
- Information entropy
- Probability theory
- Pseudorandomness
- Pseudorandom number generator
- Random number
- Random sequence
- Random variable

- Randomization
- Stochastic process
- White noise

Misconceptions/logical fallacies

Main article: Gambler's fallacy

Popular perceptions of randomness are frequently wrong, based on logical fallacies. The following is an attempt to identify the source of such fallacies and correct the logical errors.

A number is "due"

This argument is that "in a random selection of numbers, since all numbers will eventually appear, those that have not come up yet are 'due', and thus more likely to come up soon." This logic is only correct if applied to a system where numbers that come up are removed from the system, such as when playing cards are drawn and not returned to the deck. In this case, once a jack is removed from the deck, the next draw is less likely to be a jack and more likely to be some other card. However, if the jack is returned to the deck, and the deck is thoroughly reshuffled, a jack is as likely to be drawn as any other card. The same applies in any other process where objects are selected independently, and none are removed after each event, such as the roll of a die, a coin toss, or most lottery number selection schemes. Truly random processes such as these do not have memory, making it impossible for past outcomes to affect future outcomes.

A number is "cursed" or "blessed"

See also: Benford's law

In a random sequence of numbers, a number may be said to be cursed because it has come up less often in the past, and so it is thought that it will occur less often in the future. A number may be assumed to be blessed because it has occurred more often than others in the past, and so it is thought to be likely to come up more often in the future. This logic is valid only if the randomisation is biased, for example with a loaded die. If the die is fair, then previous rolls give no indication of future events.

In nature, events rarely occur with perfectly equal frequency. So observing outcomes to determine which events are likely to have a higher probability, makes sense. It is fallacious to apply this logic to systems which are designed so that all outcomes are equally likely, such as shuffled cards, dice and roulette wheels.

Books

- *Randomness* by Deborah J. Bennett. Harvard University Press, 1998. ISBN 0-674-10745-4.
- *Random Measures, 4th ed.* by Olav Kallenberg. Academic Press, New York, London; Akademie-Verlag, Berlin, 1986. MR0854102.
- *The Art of Computer Programming. Vol. 2: Seminumerical Algorithms, 3rd ed.* by Donald E. Knuth. Reading, MA: Addison-Wesley, 1997. ISBN 0-201-89684-2.
- *Fooled by Randomness, 2nd ed.* by Nassim Nicholas Taleb. Thomson Texere, 2004. ISBN 1-58799-190-X.
- *Exploring Randomness* by Gregory Chaitin. Springer-Verlag London, 2001. ISBN 1-85233-417-7.

- *Random* by Kenneth Chan includes a "Random Scale" for grading the level of randomness.

See also

- Aleatory
- Frequency probability
- Chaitin's constant
- Probability interpretations
- Nonlinear system

References

1. ^ Third Workshop on Monte Carlo Methods, Jun Liu, Professor of Statistics, Harvard University
2. ^ Municipal Elections Act (Ontario, Canada) 1996, c. 32, Sched., s. 62 (3) : "If the recount indicates that two or more candidates who cannot both or all be declared elected to an office have received the same number of votes, the clerk shall choose the successful candidate or candidates by lot."
3. ^ *Handbook to life in ancient Rome* by Lesley Adkins 1998 ISBN 0195123328 page 279
4. ^ *Religions of the ancient world* by Sarah Iles Johnston 2004 ISBN 0674015177 page 370
5. ^ *Annotated readings in the history of statistics* by Herbert Aron David, 2001 ISBN 0387988440 page 115. Note that the 1866 edition of Venn's book (on Google books) does not include this chapter.
6. ^ "Each nucleus decays spontaneously, at random, in accordance with the blind workings of chance". *Q for Quantum*, John Gribbin
7. ^ Breathnach, A. S. (1982). "A long-term hypopigmentary effect of thorium-X on freckled skin". *British Journal of Dermatology* **106** (1): 19–25. doi:10.1111/j.1365-2133.1982.tb00897.x. PMID 7059501. "The distribution of freckles seems to be entirely random, and not associated with any other obviously punctuate anatomical or physiological feature of skin.".
8. ^ Are the digits of pi random? researcher may hold the key.
9. ^ Donald Knuth, "Things A Computer Scientist Rarely Talks About", Pg 185, 190-191, CSLI
10. ^ Terry Ritter, Randomness tests: a literature survey. http://www.ciphersbyritter.com/RES/RANDTEST.HTM

External links

- An 8 foot tall Probability Machine (named Sir Francis) comparing stock market returns to the randomness of the beans dropping through the quincunx pattern. from Index Funds Advisors IFA.com
- QuantumLab Quantum random number generator with single photons as interactive experiment.
- Random.org generates random numbers using atmospheric noises (see also Random.org).
- HotBits generates random numbers from radioactive decay.
- QRBG Quantum Random Bit Generator
- Chaitin: Randomness and Mathematical Proof
- A Pseudorandom Number Sequence Test Program (Public Domain)
- *Dictionary of the History of Ideas*: Chance
- Philosophy: Free Will vs. Determinism
- RAHM Nation Institute
- History of randomness definitions, in Stephen Wolfram's *A New Kind of Science*
- Computing a Glimpse of Randomness

Categories: Cryptography | Probability and statistics | Randomness